The One-Hour Security Plan: How the University of Arizona Achieved 1,002% ROI with Sibylity

Executive Summary

When the University of Arizona discovered their small cybersecurity team could only maintain risk-informed security plans for just a handful of the most critical resources, leaving most of their institution invisible and unmanaged, they faced a harsh reality. Comprehensive coverage using traditional methods would theoretically cost $2.57 million they didn't have. Rather than accept these blind spots, they partnered with SibylSoft to completely transform their approach. The results were extraordinary: from less than 12 security plans to almost 300, from near-zero visibility to 100% participation, and from an impossible expense to a program generating $3.9 million in annual value with a 1,002% ROI.

The Challenge: A Broken Model at Breaking Point

By 2018, the University of Arizona's cybersecurity program had reached a critical inflection point. Like many large institutions, they were struggling with the complexity of managing risk across a decentralized environment.

The Scale of the Problem

The University encompassed over 100 distinct units, each managing multiple systems, applications, and data repositories. Their existing approach involved distributing lengthy compliance questionnaires every one to three years, and it had become an expensive exercise that barely scratched the surface of their actual risk landscape.

The Harsh Reality:

- **Less than a dozen security plans** actively maintained across the entire institution.
- **16-40 hours required,** per participant, to create a single security plan.
- **Massive blind spots**: The team had little visibility into distributed resources.
- **Shadow IT everywhere**: Many acquisitions occurred outside official channels.
- **Impossible economics**: Full coverage using traditional methods would theoretically cost $2.57 million annually; budget the University couldn't justify.

"**Before UASecure, we were based around a spreadsheet-based system,**" recalls Steve Hicks, Principal Information Security Architect. "**With over 100 units, everybody trying to manage spreadsheets and very few people at the ISO driving the process, it was patchy, participation was low, and it was very difficult and time consuming.**"

The Breaking Point

The University faced an impossible choice: continue with minimal coverage and accept massive risk exposure, or somehow find $2.57 million annually to achieve comprehensive security planning; money that was anticipated to deliver an estimated risk reduction value of only $943,740.

The stark truth: They weren't choosing between partial and full coverage. They were operating nearly blind, with the security team lacking bandwidth to see beyond a tiny fraction of their risk landscape. Something had to fundamentally change.

The Solution: A Revolutionary Approach

Rather than tweaking their existing model, the University of Arizona chose complete transformation. They partnered with SibylSoft to build their program around Sibylity, the first AI-driven workflow and gamified collaboration platform that helps resource teams participate in cyber risk management and security planning while the security team has full visibility and control. It decentralizes work traditional GRC tools don't; clearing bottlenecks and ending the triage created by fully centralized approaches.

The New Paradigm

The transformation centered on these strategic pillars:

1. **Value-Focused Approach**: At the heart of Sibylity is a relentless focus on value-adding activities and the elimination of waste.
2. **Embedded Expertise (Knowledge Bridge)**: Sibylity addresses the fundamental challenge in this new risk management paradigm: how to provide security expertise to resource teams at the point of decision-making.
3. **Automation for Efficiency**: Leveraging AI and automation to reduce manual effort and improve consistency across the institution.
4. **Psychological Safety**: Creating an environment where teams feel safe being honest about gaps, focusing on positive reporting and collaborative problem-solving.
5. **Engagement Through Gamification**: Using role-specific challenges, competitions, and achievements to sustain participation and build security champions.

How Sibylity Works

The platform delivers these principles through concrete features and capabilities, including:

- **AI-Powered Risk Analysis**: Thia (the hybrid AI platform) automatically analyzes resource profiles and suggests relevant risks and mitigations ranked by impact
- **Automated Security Plan Generation**: Creates comprehensive, actionable security plans using insights from resource-specific cyber risk management activities
- **Control Inventory Management**: One-time documentation of controls that persists year-to-year, replacing redundant questionnaires with continuous improvement

- **Common Control Sharing**: Service providers document controls once and share them across all dependent resources
- **Multi-Framework Compliance Mapping**: Same controls map to multiple frameworks (NIST, ISO, HIPAA, etc.) without duplicate work
- **Just-in-Time Guidance**: Context-sensitive help and expertise delivered exactly when users need to make decisions

"**One benefit of our hybrid AI approach is that we use the right tool for each need; no more, no less,**" explains Sonya Lowry, former Director of Cybersecurity Compliance at UA and current President of SibylSoft. "**It's like choosing the right tool for the job instead of swinging a sledgehammer at a finishing nail.**"

Transformational Results: By the Numbers

The University of Arizona's bold approach delivered outcomes that redefined what's possible in institutional cybersecurity; taking them from near-zero visibility to comprehensive coverage.

Financial Impact

From Impossible to Achievable

- **Before Sibylity**: Less than 12 security plans were consistently maintained (theoretical cost for full coverage: $2.57M)
- **After Sibylity**: Almost 300 active security plans for a total cost under $360,000 annually (includes software costs and labor combined)
- **Reality**: The University achieved something that was financially impossible before

93.75% Reduction in Labor Requirements

- Before: 16+ hours per participant per security plan
- After: 1 hour per participant per security plan
- Result: Made comprehensive planning feasible for the first time

1,002% Return on Investment The program generates $3.9 million in annual value through three key areas:

- **Risk Reduction**: $943,740 in direct annualized loss expectancy reduction

- **Efficiency Gains**: $2.38 million saved by reducing the effort required for both security team and resource team members
- **Strategic Value**: $582,120 in security team capacity now available for proactive and strategic initiatives

45-Day Payback Period The transformation paid for itself in just over six weeks; transforming an impossible expense into a viable security investment.

Beyond the financial fundamentals, the comprehensive visibility and maturity achieved through the transformation enabled critical business outcomes. **"A big part of why we were able to get ransomware coverage was explaining to our insurance company what we had in terms of a federated approach to cybersecurity across the organization,"** notes Steve Holland, Chief Risk Officer.

Cultural Transformation

Perhaps the most significant achievement was the fundamental shift in how the University approaches cybersecurity; moving from a compliance-driven burden to a collaborative, organization-wide commitment.

From Adversarial to Collaborative "Before UASecure, I had concerns about the risk invisibility into my organization," shares Dirk Timmerman, Director of IT for the College of Public Health. "I didn't feel that, after those were submitted, we really got the feedback and follow-up that were needed to make a difference. And that's what I think we get now—beneficial feedback that says we're on the right path."

From Reactive to Proactive Resource teams began engaging security early in project lifecycles, preventing costly retrofits and reducing implementation friction. Security conversations evolved from "what's required" to "what's possible."

From Isolated to Integrated "When it comes to cybersecurity management, one of the biggest concerns is not even being aware that a risk exists," explains Lizeth Mora, Senior Director of IT for the College of Social & Behavioral Sciences. "It's keeping us organized and focused on finding the right solutions when we have a problem."

Building Security Champions: The gamification elements and positive reinforcement approach transformed resource owners from reluctant participants to security champions.

"If we have everybody at the university participating and keeping cyber-risk top-of-mind, then those people are in a better position to make risk-informed decisions," emphasizes Brendan Miller, Director of Governance, Risk, and Compliance.

Implementation Journey: From Vision to Reality

Phase 1: Foundation Building

The University began with forward-thinking early adopter departments who helped refine both the platform and processes. These pioneers provided critical feedback and early success stories.

Phase 2: Strategic Expansion

Building on early wins, the program expanded in carefully managed waves. Each expansion phase incorporated lessons learned and provided adequate support for new participants.

Phase 3: Institutional Scale

As word spread about the platform's effectiveness and ease of use, adoption accelerated organically. A community of practice emerged, with resource teams sharing best practices and supporting peers.

Key Lessons Learned

- **Executive Sponsorship with Organic Growth**: Leadership commitment from the CISO provided necessary resources, while grassroots initiatives fueled acceleration.
- **User-Centric Design**: Resource teams often have no prior experience managing cyber risk. The best results come when tools are designed and tested accordingly.
- **Technology Enables, Culture Delivers** Sibylity's AI-powered platform was crucial in enabling the cultural transformation that determined success; shifting ownership, building trust, and fostering collaboration.
- **Perfect Is the Enemy of Good** The "One-Hour Security Plan" isn't about shortcuts; it's about starting. By capturing what's known and identifying gaps transparently, the University built momentum for continuous improvement.
- **Distributed Responsibility Works** When given the right tools and support, resource teams proved capable of managing their own cybersecurity; often better than centralized teams could in the time they had available.

"Effective risk management is not just about preventing threats—it's about empowering the organization to confidently navigate uncertainty, protect its assets, and thrive in a constantly evolving digital landscape," advises Timothy Schwab, CISO of the University of Arizona.

Conclusion: An End to Security Theater

The University of Arizona's journey represents something far more profound than cost savings or efficiency gains. They transformed from maintaining fewer than a dozen security plans, flying blind across 90+% of their institution, to achieving comprehensive coverage of nearly 300 resources, and growing, with 100% unit participation.

This wasn't optimization. It was a revolution.

Before Sibylity, the University faced an impossible equation: comprehensive security planning would theoretically cost $2.57 million they didn't have, to deliver less value than the cost. So they did what most institutions do; they managed what little they could and hoped for the best.

Today, they've achieved what was literally impossible under the old model:

- **100% participation** across all units
- **93.75% reduction** in time requirements
- **$3.9 million** in annual value creation
- **45-day** payback period
- A culture where security is everyone's responsibility

Most importantly, the University demonstrated that this transformation is repeatable. The model they pioneered can work for any organization willing to challenge the status quo.

"It's great. I don't have to spend much time after the initial questionnaire to know what I'm doing, know what I'm focusing on, know what the issues are. So, I love it!" says Mario Uribe, IS & Risk Assessment Manager for the College of Medicine.

The question for other institutions isn't whether they can afford to transform their cybersecurity programs—it's whether they can afford not to.

About Sibylity

Sibylity is the first AI-driven workflow and gamified collaboration platform that helps resource teams participate in cyber risk management and security planning while the security team maintains full visibility and control. It decentralizes work traditional GRC tools don't—clearing bottlenecks and ending the triage created by fully centralized approaches.

Born from the University of Arizona's pioneering transformation, Sibylity fundamentally reimagines how organizations manage cybersecurity risk by making it possible for those closest to the systems to manage their own security with AI-powered guidance every step of the way.

About SibylSoft

SibylSoft is the innovative provider behind its flagship platform, Sibylity. With a mission to enable organizations to build stronger, more resilient cybersecurity postures through collaboration, stakeholder empowerment, and AI-driven automation, SibylSoft makes it possible for organizations of all sizes to implement shared responsibility approaches and realize the benefits of more collaborative, context-aware cybersecurity practices.

LEARN MORE